FBK | CS
cybersecurity

Об интегральных показателях защищенности и приведении к ним результатов проверок

Курило АП,
ктн. Доцент РГУ им.Губкина,
Советник по ИБ ООО «Финансовые и бизнес консультанты» (ФБК)
Советник по ИБ ООО ФБК CS

Банное-
Юбилейный 2024

Чем достигается хороший результат?

Эффективным управлением (*качественным воздействием* на объект управления) и эффективным контролем (*качественной обратной связью* в контуре управления объекта).

Чем обусловлено качество?

- правильным выбором точек воздействия и контролируемых параметров
- правильным выбором метрик измерения
- полнотой контроля
- своевременностью реакции на отклонения
- адекватностью управляющего действия

Проверка - основная форма контроля

FBK | CS
cybersecurity

Причины происходящего

Доминирующий взгляд на защиту информации как на стационарный процесс реализации требований по защите сформировался в середине 80-хгодов прошлого века и безнадежно устарел.

Система обеспечения информационной безопасности в стране в целом требует серьезного обновления и централизации, замены идеологии «регулирования» на идеологию «управления».

Следствие происходящего.
Сколько уже сейчас разных проверок на практике?

- 14, не считая выполнения Указа Президента №250 в части импротозамещения и целевых проверок ФСБ.

- Плюс проверки отраслевых регуляторов

- **И это не финал. Есть отчетливая тенденция к увеличению числа таких проверок»!**

Централизованное планирование, координация и учет данных отсутствует

FBK | CS cybersecurity

Причины роста числа проверок

- Отсутствие достаточной координации между регуляторами в части единой согласованной методологии проверок, фиксации, представления, обработки и интерпретации результатов проверок
- Отсутствие достаточного объема информации о состоянии защищенности объекта в результатах каждой проверки, неопределенность
- Желание каждого регулятора и инициативного ФОИВ организовать собственные проверки
- Наличие положительного эффекта от любой, даже самой экзотической проверки
- Высокая неопределенность реальной защищенности в межпроверочный период
- Низкий уровень доверия со стороны регуляторов к результатам проверок, выполненных «посторонними» организациями

О том, в какое положение попадают объекты защиты и их коллективы, никто не думает.

Направления и периодичность проверок

1	**Контроль соответствия требованиям по защите (ФЗ, ГОСТ, НПА ФСТЭК и ФСБ, Минцифры, РКН) и общей организации работ** • **полная** • **Выборочная**	**3 года** **1 год**
2	Контроль настроек средств защиты • техническими средствами • организационными средствами	1-3 года
3	Проверка готовности объекта в целом к отражению атак (киберучения)	Не определено нормативно
4	Выявление уязвимостей: • инструментальными методами • аналитическим методами	Не определено на федеральном уровне
5	Мониторинг вторжений и аномалий	Непрервывно

Направлений пять, проверок восемь, остальные, существующие на практике - производные

№ п/п	Вид контроля	Что преимущественно оценивается	Форма измерения, состояние СОИБ	Результативность
1	**Аттестация**	Выполнение требований ФСТЭК	Дискретная, статическое	Не высокая
2	**Аудит ИБ**	Общее состояние системы защиты, организация работ, выполнение требований по защите	Дискретная, статическое	Средняя Не закрывает проблему реальной защищенности
3	**Оценка соответствия требованиям по безопасности**	Соответствие заданным требованиям по безопасности	Дискретная, статическое	Выше средней Не закрывает проблему реальной защищенности
4	**Оценка безопасности КИИ**	Анализ деятельности по отражению кибератак	Дискретная, статическое. Анализ логов состояния на момент атаки	?
5	**Госконтроль**	Выполнение требований ФЗ и ФСТЭК	Дискретная, статическое	Аналог аудита
6	**Экспресс-оценка защищенности**	Требования по безопасности для отдельных элементов СОИБ,	Дискретная, статическое	Противоречит сложившейся идеологии
7	**Инструментальное тестирование**	Наличие уязвимостей в системе	Дискретная, статическое	Высокая
8	**Белый хакинг**	Наличие уязвимостей в системе	Статическое, в течение длительного времени	Возможны серьезные негативные последствия
9	**Мониторинг СОИБ. Мониторинг настроек СИБ**	Текущее состояние защищенности и состояния системы	Непрерывная, динамическое	высокая
10	**Мониторинг СОИБ. Мониторинг инцидентов**	Наличие результативных атак	Непрерывная, динамическое	высокая
11	**Контрольная проверка**	Подготовленность и работоспособность коллектива	Дискретная, статическое	Низкая в части оценки требований ИБ. Высокая в части оценки деятельности коллектива
12	**Анализ рисков**	Уязвимости и ошибки в системе защиты, создающие риски ИБ	Дискретная, статическое	Высоко ресурсозатратная превентивная мера с неясной эффективностью
13	**Проверки по 152 ФЗ**	Готовность к обработке инцидентов	Дискретная, статическое	Практически не влияют
14	**Киберучения**	Реальная готовность коллектива АИС (объекта) к отражению атак	Дискретная, динамическое	Весьма высокая

Результат:

Сложно.
Огромный объем документации (до 1000 листов текста суммарно по всем проверкам)
Сумбур в представлении их результатов.
Отсутствие внятной методологии проверок.
Не дает реальной картины.
Высокие трудозатраты.

Следствие:

В стране 500 000 объектов КИИ из них 35 тыс ЗО КИИ из них 10% в реестре.
В ходе проверок ФСТЭК выявляет по 800 нарушений в год. Составлено более 160 протоколов об административных правонарушениях.
Сопоставить результаты контролей, представленных в отчетах, в настоящее время невозможно.
Дальнейшее усложнение картины и перегрузка служб ИБ.
Централизованной отчетности и нормальной статистики нет.
Риски суровых административных и дисциплинарных санкций для персонала ИБ.
Дальнейшая децентрализация в управлении системой.

FBK | CS cybersecurity

Вопросы -ответы

14 видов контролей на один объект это не слишком ли много? Можно ли избавиться от некоторых?	• Радикально сократить невозможно. • Нужно их сократить по общему основанию (до 5 направлений) и не плодить новые сущности
Можно ли верить оценщику?	• Пока доверия нет. • В принципе вопрос повышения доверия к оценщику решаем
Не слишком ли длинный цикл оценки (до 3 лет)?	Цикл статических оценок сократить невозможно, они весьма ресурсозатратны. При этом, они не отражают текущий уровень защиты и состояние объекта в межпроверочный период.
Какова точность оценок, почему ситуация не улучшается?	• Разная, более конкретных оценок нет. • Отсутствуют общеметодологический и общеметодический подходы. • Плохо совершенствуется система защиты из за противоречий интересов и целей бизнеса и безопасности.
Как свести показатели полученные по разным проверкам какому то внятному показателю?	• Нужна единая система оценок, опирающаяся на общепринятые комплексные показатели состояния объекта защиты, (с оценкой результатов контроля и тестирования, а также степени зрелости процессов СОИБ)

Первый и главный шаг в повышении качества управления СОИБ – организация сбора и обработки отчетности

1. **Привести результаты всех имеющихся контролей к стандартному унифицированному виду**, позволяющему централизованно, собирать, хранить и обрабатывать информацию, исключить дублирование проверок, а также обеспечить доступ к результатам заинтересованных субъектов (регуляторов и их представителей).
2. **Использовать как унифицированный подход методологию оценки зрелости процессов обеспечения СОИБ для каждого объекта защиты**.
3. **Ввести реестры процессов обеспечения СОИБ для каждого объекта** как основу (классификатор) методик проверки, анализа и экспертизы.
4. **Ввести обязательный централизованный сбор (представление) отчетности** от всех контролируемых объектов защиты и сбор отчетности об устранении выявленных недостатков и контроле (самооценке) показателей зрелости процессов обеспечения СОИБ.

Под процессом обеспечения СОИБ следует понимать целенаправленную деятельность по обеспечению выполнение требований по безопасности и достижения установленных показателей уровня защищенности

Прежде чем браться за модернизацию системы контроля и отчетности нужно уточнить следующее

1. Что такое защищенность ИБ, как она соотносится н новомодным термином «кибербезопасность» и защищенность чего мы оцениваем.
2. Как ведет себя это свойство, от чего зависит. Каковы факторы (составляющие), существенно влияющие на защищенность.
3. Как оценить защищенность.
4. Можно ли верить результатам контроля, каковы условия доверия.
5. Как повысить доверие.
6. Что такое интегрированный показатель защищенности и можно ли его ввести.
7. Как свести результаты разных видов контроля к виду, который можно оценивать и сравнивать.
8. Нужна ли система сбора отчетности по результатам контроля. Какая она должна быть.
9. Равноценны ли требования по защите или есть группа наиболее важных, дающих 80% результата?

Возможный общеметодологический подход

1. Использование для представления результатов оценок методологии построения модели зрелости **процессов обеспечения СОИБ** и соответствующей шкалы.
   - *Процессы могут включать в себя подпроцессы.*
   - *Модель зрелости и шкала оценки процессов обеспечения СОИБ хорошо известны и строятся на базе группы стандартов ГОСТ Р 15504 и стандарта COBIT 4.1.*
2. Все оцениваемые процессы обеспечения СОИБ объекта идентифицируются, им присваиваются соответствующие метрики, устанавливаются критерии защищенности. Процессы включаются в реестр процессов объекта. Каждое установленное нормативно требование или группа требований по защите соотносится с соответствующим процессом.
3. Результаты оценки по любой методике привязываются к соответствующим процессам и оцениваются по шкале зрелости. Интегрированные результаты оценки по шкале зрелости показывают уровень состояния работ по обеспечению информационной безопасности.
4. Результаты проверки, интерпретированные в универсальную форму оценки, в обязательном порядке направляются в единую базу данных отчетности.
5. В центральной базе данных информация представлена в форме, позволяющей проводить глубокие аналитические исследования и делать боле точные, чем сейчас оценки.

Что оценивается

Итоговое состояние защищенности объекта оценивается интегральными показателями, характеризующими:

- качество управления СОИБ
- качество реализации защитных мер
- качество контроля деятельности, в том числе и мониторинга, а также систем защиты

Как оценивается

Компиляция линейной шкалы зрелости процесса
и циклических механизмов PDCA

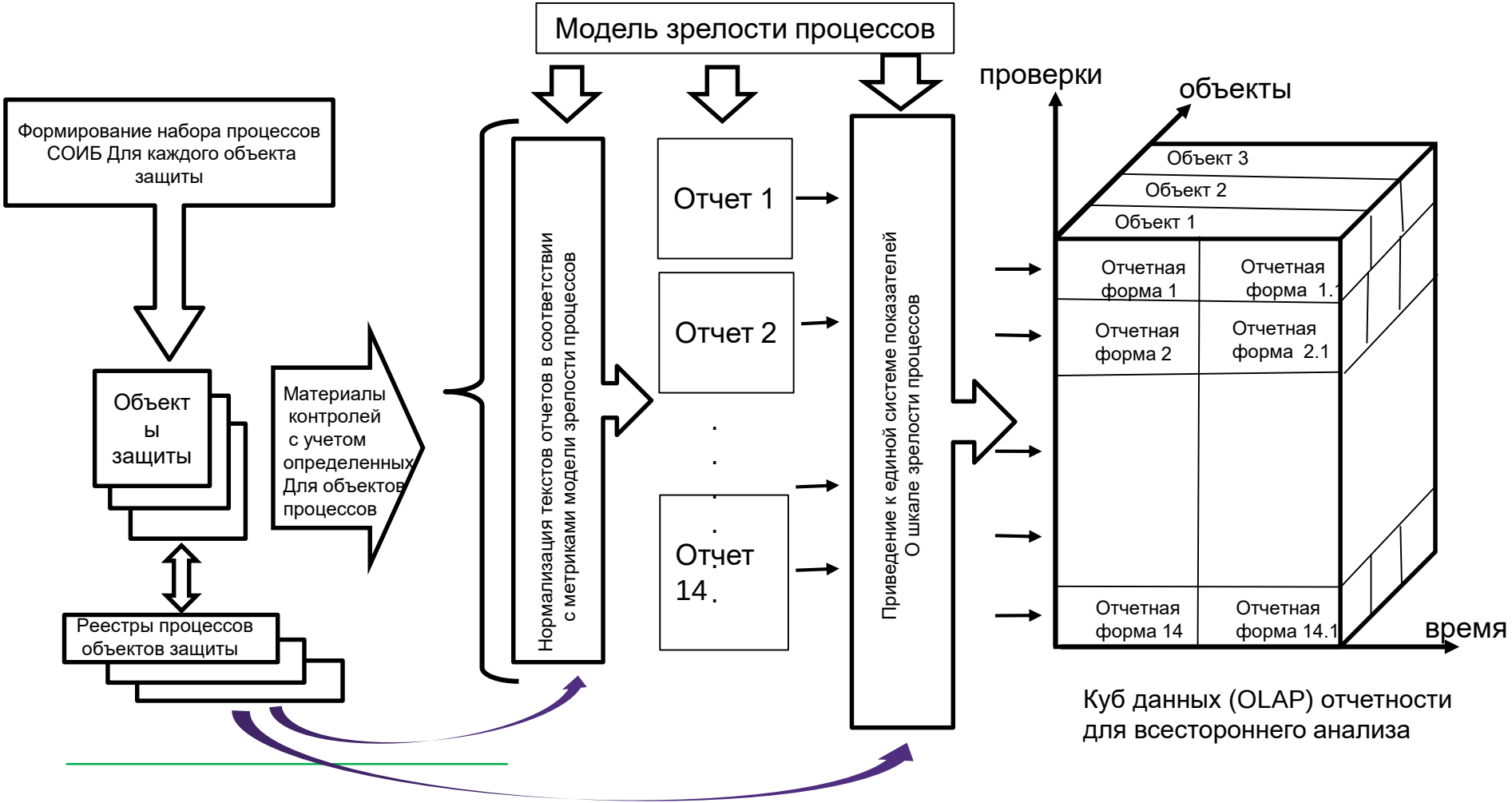
Направления оценки

1. Выполнение требований законодательства и НПА регуляторов.
   - полная проверка
   - проверка выполнения критических (наиболее важных) требований
2. Соответствие настроек СОИБ установленным требованиям по защите
3. Наличие уязвимостей:
   - инструментальный контроль
   - аналитический контроль
4. Готовность к реальному отражению атак (киберучения).
5. Деятельность по мониторингу вторжений и аномалий, менеджмент инцидентов.

Результат и новые возможности

1. Консолидация результатов проверок
2. Снижение объема проверок, планирование
3. Точное знание состояния объектов защиты, как самой службой ИБ, так и регуляторами
4. Возможность всестороннего анализа результатов проверок
5. Возможность использования собираемой информации в интересах всех регуляторов

Пример схемы формирования интегрированной отчетности



Куб данных (OLAP) отчетности для всестороннего анализа

Следует рассматривать описание защищенности объекта защиты в форме многомерного информационного куба (OLAP), каждая ячейка которого содержит информацию о проведенном контроле (реализуемом процессе) и их результатах. Результаты представляются по шкале оценки зрелости на основе методологии построения модели зрелости процессов.

FBK | CS
cybersecurity

Контакты

Андрей Курило
Советник по вопросам информационной безопасности

+7 (495) 737 53 53 доб. 3037

+7 (495) 970-41-32
Sales@fbkcs.ru
Info@fbkcs.ru